PATENT ABSTRACTS OF JAPAN

(11)Publication number : 2000-076789
(43)Date of publication of application : 14.03.2000

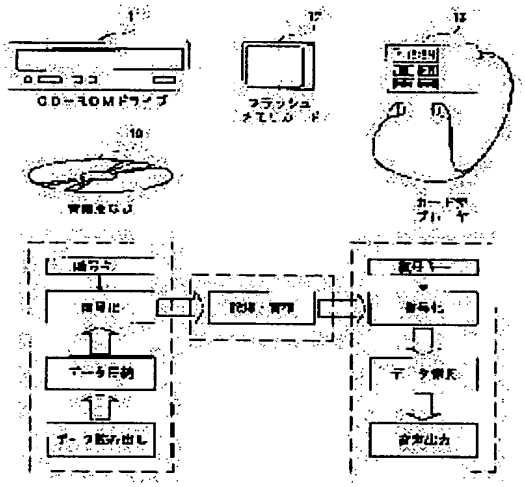
(51)Int.CI. G11B 20/10
G06F 12/14

(21)Application number : 10-249302
(22)Date of filing : 03.09.1998

(71)Applicant : HITACHI LTD
(72)Inventor : TSUJIMURA HIROFUMI

(54) ENCODED SOUND REPRODUCING SYSTEM FOR CD LINEAR PCM DATA

(57)Abstract:
PROBLEM TO BE SOLVED: To use the copied CD musical data only for a CD owner by providing a means encoding the CD linear PCM data with an optical storage and decoding the data with a sound reproducing device, and also providing a setting means of an encoding/decoding key and a storage means of a key in respective devices.
SOLUTION: The linear PCM data in a musical CD 10 are read out by a CD-ROM drive 11, and are compressed/encoded to be transferred onto a main memory of a personal computer main body. The encoded CD data are copied onto a flash memory card 12 in a regular file form by a card drive loaded on the personal computer. The card 12 is used by being loaded on a portable type card type player 13. In the card type player 13, the data are read out from the card 12, and are decoded, and expanded further to be returned to the linear PCM data. The linear PCM data are made an audio analog signal by a digital analog converter to be outputted as music by an earphone, etc.



LEGAL STATUS

[Date of request for examination] 02.07.2003

[Date of sending the examiner's decision of rejection]

[Kind of final disposal of application other than the examiner's decision of rejection or application converted registration]

[Date of final disposal for application]

[Patent number]

[Date of registration]

[Number of appeal against examiner's decision of rejection]

[Date of requesting appeal against examiner's

(19)日本国特許庁（ＪＰ）　(12) **公開特許公報（Ａ）**　(11)特許出願公開番号
特開2000－76789
（P2000－76789A）
(43)公開日　平成12年３月14日(2000.3.14)

(51)Int.Cl.'	識別記号	ＦＩ		テーマコード'（参考）
Ｇ１１Ｂ　20/10		Ｇ１１Ｂ　20/10	Ｈ	５Ｂ０１７
Ｇ０６Ｆ　12/14	３２０	Ｇ０６Ｆ　12/14	３２０Ｂ	５Ｄ０４４

審査請求　未請求　請求項の数９　ＯＬ　（全　９　頁）

(21)出願番号　特願平10－249302

(22)出願日　平成10年９月３日(1998.9.3)

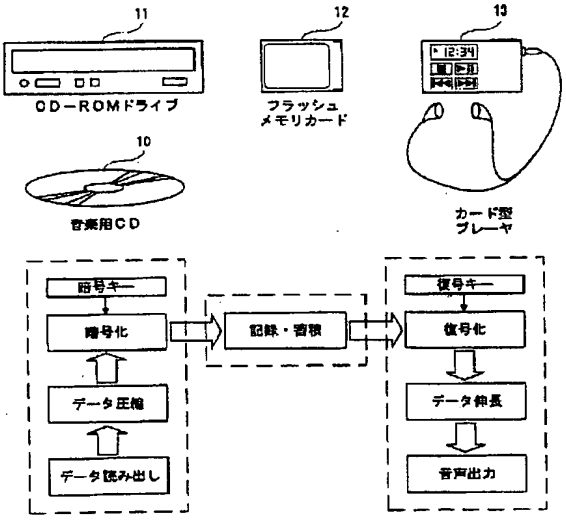
(71)出願人　000005108
株式会社日立製作所
東京都千代田区神田駿河台四丁目６番地
(72)発明者　辻村　宏文
神奈川県横浜市戸塚区吉田町292番地　株式会社日立製作所映像情報メディア事業部内
(74)代理人　100068504
弁理士　小川　勝男

Ｆターム(参考)　5B017 AA06 BA07 BB03 CA09
5D044 AB05 BC03 CC04 DE50 GK08
GK17 HL08 HL11

(54)【発明の名称】　ＣＤリニアＰＣＭデータの暗号化音声再生システム

(57)【要約】
【課題】著作物であるＣＤ音楽データの取り扱いを、一般のデジタルデータと同じように簡単に、データファイル形式で複製や蓄積や転送ができるようにする。
【解決手段】暗号・復号化キーを、光ストレージ装置側と音声再生装置側とで共有し設定記憶する手段を設け、暗号化されたＣＤ音楽データファイルはシステム内でのみ有効な再生ができるようにする。

図　1



1

【特許請求の範囲】

【請求項１】ＣＤ（コンパクトディスク）リニアＰＣＭデータを読み出し可能な光ストレージ装置（以下、Ｓ装置）と、デジタルデータから音声アナログ信号への変換を行う音声再生装置（以下、Ｄ装置）との関係において、

これら２つの装置間に、データの蓄積や転送や複製が可能な装置が存在し、この装置を介する経路（以下、開いた経路）を通して、ＣＤリニアＰＣＭデータを受け渡す場合に、

(1) 予め、Ｓ装置とＤ装置の間で暗号・復号化キーの共有を行い、それぞれの装置内に、このキー情報を記憶しておき、(2) Ｓ装置でリニアＰＣＭデータを暗号キーにより暗号化してデータを出力し、(3) 開いた経路を通して、(4) Ｄ装置で暗号化されたデータを復号キーにより元のリニアＰＣＭデータに変換し音声信号として出力することを特長とするＣＤリニアＰＣＭデータの暗号化音声再生システム。

【請求項２】請求項１のシステムにおいて、Ｓ装置での暗号化の前にデータ圧縮を施し、Ｄ装置で復号後にデータ伸長を施すことを特徴とする請求項１記載のＣＤリニアＰＣＭデータの圧縮暗号化音声再生システム。

【請求項３】請求項１又は請求項２のシステム機能を実現するために、キーの記憶手段と暗号化手段を有することを特徴とする請求項１記載のＣＤリニアＰＣＭデータの暗号化音声再生システム装置。

【請求項４】請求項１または請求項２のシステム機能を実現するために、キーの記憶手段と復号手段を有することを特徴とするＣＤリニアＰＣＭデータの暗号化音声再生システム装置。

【請求項５】請求項１または請求項２のシステムにおいて、暗号・復号キーの共有化に際し、Ｓ装置とＤ装置を直接ケーブルで接続して、キーの受け渡しを行うキーの配信方式であることを特徴とするＣＤリニアＰＣＭデータの暗号化音声再生システム。

【請求項６】請求項１または請求項２のシステムにおいて、パーソナルコンピュータに接続されるＳ装置、Ｄ装置に対して共通の暗号・復号キーをオペレーティングシステムが配信する配信方式であることを特徴とするＣＤリニアＰＣＭデータの暗号化音声再生システム。

【請求項７】請求項１または請求項２のシステムにおいて、デジタル情報記録媒体の再生機能を有するＤ装置に対して、パーソナルコンピュータに接続された同種のデジタル情報記録媒体の記録再生装置で、キー情報およびキーの書き換えを要求する情報を含む記録媒体を作成し、Ｄ装置にキーを配信するキーの配信方法であることを特徴とするＣＤリニアＰＣＭデータの暗号化音声再生システム。

【請求項８】請求項１または請求項２のシステムにおいて、Ｄ装置において、再生時間や再生回数などをカウント記憶し、一定時間または一定回数に達した場合に、キーの書き換えを要求することを特徴とするＣＤリニアＰＣＭデータの暗号化音声再生システム。

2

【請求項９】請求項１または請求項２のシステムにおいて、暗号キーと複号キーを共通として、少なくとも、Ｓ装置が発生した乱数ビット列と、Ｄ装置が発生した乱数ビット列と、のどちらかを含む乱数ビット列を共通のキーとして定義し、Ｓ装置またはＤ装置が、配信されたキーのビット列の内部に自装置の発生させた乱数ビット列が存在しない場合に、不正キーとみなしてキーの記憶設定を拒否することを特長とするキーの生成方式およびキーの認証方式であることを特徴とするＣＤリニアＰＣＭデータの暗号化音声再生システム。

【発明の詳細な説明】

【０００１】

【発明の属する技術分野】パーソナルコンピュータを中核とする音声再生システムでのＣＤリニアＰＣＭデータの取り扱いに関する。

【０００２】

【従来の技術】パーソナルコンピュータ（以下、パソコン）の周辺装置であるＣＤ－ＲＯＭドライブや、ＤＶＤドライブなどの光ストレージ装置（以下、単に「ドライブ」と略す）は、音楽用ＣＤの再生も可能である。しかし、ＣＤに記録されている音楽データはリニアＰＣＭのデジタルデータであるが、一般のＣＤ－ＲＯＭディスクやＤＶＤディスクに記録されているデジタルデータとは扱いが異なり、ドライブからリニアＰＣＭデータを取り出すことは制限されている。これはＣＤ音楽の著作権保護（不正コピーの防止）のためである。

【０００３】このため現状のパソコン上での音楽ＣＤの再生は、ドライブが直接出力するアナログ信号を、サウンドカードのミキシング回路を経由してスピーカから聞くか、あるいはドライブのフロントパネルに配置された音声出力端子からイヤホンや外部スピーカで聞く、という方法が採られている。

【０００４】パソコン内蔵型のＣＤ－ＲＯＭドライブでは、取り外しの必要がないためアナログ信号線を直接サウンドカードに接続することは問題が無い。しかし、ノート型パソコン用のポータブルＣＤ－ＲＯＭドライブなどの、いわゆる外付けドライブでは、ＳＣＳＩなどの標準的なデジタル信号ケーブルに加えて、アナログ信号線が必要となっている。あるいは、標準のデジタル信号にアナログ信号を付加した専用ケーブルが必要となっている。

【０００５】ＣＤリニアＰＣＭデータは、同じデジタルデータであるにも関わらず、ハードディスク等の別の記録再生装置にデータファイルとして複製することはできない。ただし、ＣＤリニアＰＣＭデータをデジタルデータとして読み出す機能を有するドライブにおいて、専用のアプリケーションプログラムを使用しデータを読み出

して、サウンドファイルとしてハードディスク等に保存することはできる。これはデータの複製（コピー）ではなく録音（レコード）という形式を取っている。

【０００６】一方、コンポーネントステレオや専用のＣＤプレーヤや、ＣＤ再生が可能なＶＣＤプレーヤやＤＶＤプレーヤなどの、専用のＡＶシステムにおいては、リニアＰＣＭデータはシリアルで外部へディジタル出力している。この出力フォーマットはＥＩＡＪ規格にもなっている。これをアンプユニットを経由してアナログ信号に変換して、スピーカに出力したり、携帯型プレーヤにデジタル録音したりすることが行われている。

【０００７】著作物をその所有者が個人的利用に限って一次複製を作成し使用することは認められており、携帯型のＭＤプレーヤにＣＤの音楽データをデジタルコピーして使用するなどの例がある。

【０００８】パソコンは、グラフィカルユーザーインターフェイスを有しており、非常に簡単にデジタルデータを他媒体へ複製記録することができ、またネットワークを介して他のパソコンへ転送することもできる、いわゆるオープンなシステムである。一方、専用のＡＶシステムの方は、デジタルデータが外部へ出て行くことが無く、そのシステム内部で完結しておりクローズなシステムである。

【０００９】パソコンは簡単にデジタルデータの複製や転送ができるオープンなシステムであるがため、著作物データの取り扱いには様々な制限が課せられている。パソコン上での著作物の再生の例に、ＤＶＤドライブとＭＰＥＧデコーダカード間のＤＶＤビデオストリームデータの再生がある。

【００１０】ＤＶＤビデオストリームは元々ＭＰＥＧ２方式で圧縮されているデータであり、ストリームデータはセクタ単位に部分的に暗号化されてディスクに記録されている。

【００１１】暗号化されたセクタを復号化するための復号キーはディスク内に記録されているが、これは通常のデータとしては読み出せないようになっている。

【００１２】ドライブからデコーダへキーの転送を行う際には、以下に述べる「認証」の手続きを経て復号キー自体を暗号化して受け渡す。この復号キーはオペレーティングシステムでさえ知ることができないような仕組みになっている。

【００１３】認証は、ＤＶＤドライブ側とＭＰＥＧデコーダ側に、同一の暗号変換手段を配備し、一方が発生させた乱数を相手側に送って、変換された値を返してもらい、自暗号化手段の変換値との一致を確認することによって行う。この手順をそれぞれ相互に行い、この認証手順で使用された２つの変換値を合成して、本来受け渡すべきストリームデータの復号キーをデータバス上で暗号化するためのキーとしている。これら全ての暗号化アルゴリズムは非公開となっている。

【００１４】さらに、この認証が成立しないと、ドライブからはストリームデータ自体も出力をしないようになっている。

【００１５】複号キーはドライブとＭＰＥＧデコーダの中にしか存在しないため、仮にストリームデータをハードディスクにコピーできたとしても正常な再生はできない。なお、認証と複号キーの受け渡しは、一つのタイトルの再生毎に行われている。

【００１６】

【発明が解決しようとする課題】汎用のデジタル情報記録再生装置に、オーディオ再生機能を付加して、携帯型プレーヤとして使用することが考えられる。例えば、数十～数百メガバイトの記憶容量を有するフロッピーディスクや、フラッシュメモリカードや、光磁気ディスク（ＭＯ）などの汎用のデジタルデータ記録媒体にＣＤ音楽データをコピーして、それぞれの記録再生装置で音楽再生することが可能である。

【００１７】また近い将来、パソコンを中核とするＡＶコンポーネントシステムが普及することが予想され、例えばＭＯドライブ、ＤＶＤ－ＲＡＭドライブ、ハードディスクドライブなどの大容量の記録再生装置に、ＣＤ音楽データを編集記録して使用することが考えられる。

【００１８】現状のシステムでは、著作物データの複製の作成およびその管理の責任は個人に任せられている。しかし、可撤性の媒体へのコピーが可能で、ネットワークに接続されるというパソコンのオープンな性格上、著作物であるデータの複製と管理には慎重を期す必要がある。

【００１９】携帯型プレーヤの記録媒体に、ＣＤ音楽データをパソコンのグラフィカルユーザーインターフェイスでファイルとしてコピーができれば、編集作業が簡単になって非常に便利である。

【００２０】しかし、ＣＤの生データのコピーを無条件で許可すると、レンタル店から借りてきたものをデジタルコピーしてそのまま保持していたり、知人友人にコピーして配布したり、ネットワーク上に公開するなどの違法な行為が行われてしまう可能性がある。

【００２１】すなわち、あまりに簡単にコピーが取れると著作権の意識が薄れて責任感が無くなるが、一方で実際の使用に当たっては簡単な操作が望ましい、いう矛盾が生まれる。

【００２２】本発明が解決しようとする課題は、ＣＤ音楽データの簡単なデジタルコピーの手段を提供し、同時に正規なＣＤ所有者以外に対しては、そのデータを利用できないようにすることである。

【００２３】

【課題を解決するための手段】ユーザーがデジタルデータを自由に複製、蓄積、転送できる環境下において、ＣＤリニアＰＣＭデータを暗号化して置くことである。そのために、光ストレージ装置側でＣＤリニアＰＣＭデー

タを暗号化し、音声再生装置側でこれを複号化する手段を設け、それぞれの装置に暗号・複号化キーの設定手段とキーの記憶の手段を設ける。キーの設定記憶は、基本的にはシステムが構築されたときの一度限りとし、ＣＤデータの送信の度ごとにリアルタイムで毎回行うわけではない。

【００２４】これを言い換えれば、個人が所有するシステム内の光ストレージ装置と音声再生装置との間に、暗号・複号化キーの共有という関係を付けておき、その間でやり取りされるデータは、そのシステム内でしか使用できないようにし、データの複製や蓄積や転送などを許可することである。

【００２５】ＤＶＤビデオの暗号化システムは、ディスクに含まれる情報の他媒体への複製を防止することを目的としている。このためＤＶＤディスクが存在しないと全く再生できない。

【００２６】本発明の目的は、ユーザーが特別に意識していなくとも、ＣＤの複製データの管理責任を果たせるようなシステムを提供することにあり、ＣＤデータの一次複製の使用を前提とした暗号化であり、この点がＤＶＤビデオの暗号化システムと異なる。

【００２７】元々ＣＤデータは暗号化されて記録されているわけではないため、然るべき機能を有したドライブにおいて意図的に生のデータを読み出すこともできる。そのため、厳密な暗号化の必要性はない。したがって、暗号・複号化のアルゴリズムは簡単であっても、完全に公開されていても構わない。

【００２８】暗号化をどの部分で行うかによって、以下のように２通りの手段がある。

【００２９】第１の方法は、光ストレージ装置の内部で、ハードウェア的にあるいはファームウェアマイコンがソフトウェア的に暗号化する方法である。

【００３０】第２の方法は、光ストレージ装置は、ＣＤリニアＰＣＭデータをそのまま出力し、パソコンのオペレーティングシステム（ＯＳ）のデバイスドライバ部でソフトウェア的に暗号化する方法である。この場合は、キーはＯＳが管理することになる。

【００３１】何れの方法にあってもパソコンでユーザーが自由に操作できるデータファイルの形態では暗号化されている。

【００３２】同様に複号化をどこで行うかによって、以下のように２通りある。

【００３３】第１の方法は、音声再生装置の内部で、ハードウェア的にあるいはファームウェアマイコンがソフトウェア的に複号化する方法である。

【００３４】第２の方法は、音声再生装置がパソコン内部にある場合に、ＯＳのデバイスドライバでソフトウェア的に複号化する方法である。

【００３５】ＣＤデータをリニアＰＣＭデータ形式そのままで暗号化を施してもよいが、暗号化の前にデータの圧縮を、複号化の後にデータの伸長を行うことも可能で、大容量の音楽データの記録蓄積には、この方が実用的である。この場合も、前記方法と同様に、圧縮・伸長を装置内部で行う方法と、パソコンのＯＳのデバイスドライバで行う方法とがある。

【００３６】暗号・複号キーの配信方法としては、以下のような方法がある。

【００３７】（１）光ストレージ装置と音声再生装置とが物理的に直接接続できて通信手段を持っていれば、装置間で相互に通信を行いキーを取り決め共有する。

【００３８】（２）光ストレージ装置と音声再生装置がパソコンに直接接続されて通信手段を持っていれば、パソコンが装置間の通信の仲立ちとなって取り決めたキーを配信する。

【００３９】（３）光ストレージ装置がパソコンに接続され、音声再生装置が携帯型プレーヤであってデータ記録媒体を介して間接的にシステムに組み込まれる場合は、記録媒体を通じてキー情報の受け渡しをする手段を設けておき、記録媒体によってキーの配信をする。

【００４０】簡単なデジタルコピーの手段を提供することによって発生する問題として、レンタルＣＤのデジタルコピーの長期保存を禁止する必要がある。

【００４１】このためには、定期的にキーの更新を行うことにより、保存されたデータを無効化する方法が有効である。

【００４２】これは、言わば、複製されたデジタルデータに寿命を与えることである。データ自体を劣化消滅させることはできないため、音声再生装置に、再生の回数または再生の総時間を記録する手段を設け、所定の回数または時間に達した場合に、キーの更新を要求するようにする。装置内部に記憶していたキーは、この時点で消去するなどして無効化する。これ以降、媒体に記録蓄積していたデータは全て使用できなくなる。

【００４３】データファイルに日付情報がある場合は、音声再生装置に有効期日を設定記憶して、ファイルの再生時に有効期日と比較して、キーの更新を要求する。

【００４４】携帯型プレーヤのような音声再生装置が記録媒体の再生機能しか有していなくて、記録媒体によってキーの配信を行う場合は、音声再生装置は与えられたキーを記憶するだけの受動的なキー設定となる。キー更新を行いたくない不正使用者が、キー配信用の媒体を保管しておき、前回のキーと同一のキーを再設定することが考えられる。

【００４５】これを防止するには、装置が前回のキーを記憶しておき、更新時に比較して同じであったらキー更新を拒否するという方法もあるが、２つ異なるキー配信媒体で交互にキー更新されると、この方法では効果が無い。さらに過去数回～数十回のキーを全て記憶しておき、その中の同じキーが指定されたならば、キー更新を拒否するという方法もあるが、その記憶数を超える数の

異なるキーの配信媒体を使って順次更新を行えば元のキーに戻すことが可能である。

【００４６】従って、媒体の再生機能しか有しない音声再生装置には、キーの更新のために直接パソコンと通信する手段を有することが望ましい。そして、前記の不正使用を防止するため、キーは音声再生装置が能動的に発生する必要がある。

【００４７】能動的なキーの生成方法として、暗号キーと複号キーを同一とする場合に、光ストレージ装置が発生させた乱数ビット列と、音声再生装置が発生させた乱数ビット列との、少なくともどちらかを含む乱数ビット列を共通のキーとする方法がある。それぞれの装置にキーを設定するとき、装置は自らが発生させた乱数ビット列がキーのビット列の中に含まれない場合は、正しいキーとして認めないようにする。

【００４８】媒体への記録機能を有する音声再生装置において、キーを記録媒体を介して受け渡す場合にこの方法を用いれば、以前使用していたキー配信用媒体にすり替えられても、それを検出することができるため、正しくキー更新を行うことができる。

【００４９】

【発明の実施の形態】第一の実施例

図１は、ＣＤ－ＲＯＭドライブとフラッシュメモリカードとカード型プレーヤの例である。ここで、光ストレージ装置はＣＤ－ＲＯＭドライブ１１でありパソコンに内蔵されているものとする。音声再生装置は、フラッシュメモリカード１２を記録媒体とする携帯可能なカード型プレーヤ１３である。音楽用ＣＤ１０内のリニアＰＣＭデータは、ＣＤ－ＲＯＭドライブ１１で読み出され、ドライブの内部において圧縮、暗号化され、パソコン本体のメインメモリ上に転送される。

【００５０】パソコンにはカードドライブも装備されており、暗号化されたＣＤデータを通常のファイルの形式でフラッシュメモリカード１２にコピーする。フラッシュメモリカードは可搬性の媒体であり、携帯型のカード型プレーヤ１３に装着して使用する。カード型プレーヤ１３は、フラッシュメモリカード１２からデータを読み出し、復号化され、さらに伸長されて元のリニアＰＣＭデータに戻され、デジタル・アナログ変換器でオーディオアナログ信号とされて、イヤホンなどで音楽として出力される。図中の点線は、装置間の物理的境界を示している。

【００５１】第二の実施例

図２は、パソコン内部のＣＤ－ＲＯＭドライブとハードディスクドライブとサウンドカードの例である。全てのデバイスはパソコン筐体に内蔵されているとする。ここでは、光ストレージ装置はＣＤ－ＲＯＭドライブ２１であり、音声再生装置はサウンドカード２３である。

【００５２】ユーザーがパソコンのオペレーティングシステムにおいて、ＣＤドライブの音楽ファイルをハードディスクへ複製する指示をドラッグ＆ドロップなどの操作で行う。

【００５３】音楽用ＣＤ２０内のリニアＰＣＭデータは、ＣＤ－ＲＯＭドライブ２１によって読み出され、そのままのパソコンのマザーボードのメインメモリに送られる。パソコンのオペレーティングシステム（物理的な実体はパソコンのＣＰＵ）が、このＣＤデータを圧縮、暗号化して、通常のデータファイルと同様にハードディスク２２上に記録保存する。

【００５４】次に、ユーザーがコピーされたハードディスク上のファイルに対して、音楽再生する指示をダブルクリックなどの操作で行う。データファイルは一端メインメモリ上に読み込まれ、オペレーティングシステムが、復号化、伸長して元のリニアＰＣＭデータに戻した後、サウンドカード２３に転送する。サウンドカード２３は、データをアナログ音声信号に変換して、パソコンの内部スピーカに、あるいは出力端子を介して外部オーディオ装置へ信号を送り音楽として再生する。図中の点線は、装置間の物理的境界を示している。

【００５５】この例では、オペレーティングシステムが暗号・復号化、圧縮・伸長の処理をソフトウェアで行っており、既存のＣＤ－ＲＯＭドライブやサウンドカードがそのまま使用できるという長所がある。

【００５６】図３は、暗号・復号化方法の一例である。

【００５７】３２ビットの原始多項式、G(x)=x^32+x^31+x^4+1によりＭ系列乱数ビット列を生成し、これと入力データビット列との排他的論理和３１を取り出力データビット列とする。暗号化と復号化は全く同じ手順であり、キーも同じである。乱数生成手段は３２ビットのシフトレジスタ３２と排他的論理和３３ａ，３３ｂを組み合わせたフィードバックシフトレジスタで構成３４でき、キーは３２ビットで乱数列の初期値として使用する。キーの記憶手段３５としては、例えば電源を切っても消えないＥＥＰＲＯＭなどのメモリを利用する。

【００５８】音楽再生では、早送り早戻し機能が必須である。このため、１曲のデータファイルを小さなブロック、例えば３２Ｋバイトに分割して、その単位毎に乱数値の初期化を行う方法が有効である。

【００５９】暗号化の目的が、データの機密保持ではなく、ある特定の音声再生装置でのみ使用できるデータとすることであり、このような簡単な暗号化方法でも構わない。

【００６０】ただし、その替わりにキーの管理方法が重要となる。

【００６１】図４は、暗号・復号化キーの生成と配信の方法の一例である。

【００６２】音声再生装置－甲４１と音声再生装置－乙４２と光ストレージ装置４３の例で、キーは３２ビットの共通キーとしている。

【００６３】何れかの装置から、あるいはオペレーティ

ングシステム（ＯＳ）４４から自動的に、またはユーザから、キーの更新要求が発せられると、各装置を集中管理しているＯＳが、このキー更新要求を各装置に伝える。各装置は、乱数（ここでは８ビット）を発生させＯＳに返す。ＯＳは、これら乱数ビット列を繋ぎあわせて、システムで要求される３２ビットの共通キーを生成する。３２ビットに満たない部分はＯＳが乱数を追加する。こうして出来上がったキーを各装置に配信しキーの設定すなわち不揮発性メモリへの記憶を要求する。

【００６４】各装置は、受け取った３２ビットのキーの中に、自装置で発生させた８ビットの乱数ビット列が含まれていることを確認する。含まれていれば、この新しいキーに書き換え、ＯＳに正常終了を通知する。もし含まれていなかった場合は、キーの書き換えは行わず異常終了をＯＳに通知する。ＯＳはすべての装置について正常終了を確認してキーの生成と配信の処理を終了する。異常終了があった場合は、ユーザーにその旨通知し、正しい更新手続きを促す。

【００６５】レンタルＣＤのデジタルコピーの長期保存を禁止するため、音声再生装置が定期的にキーの更新要求をする必要があり、以下のような方法がある。

【００６６】ファイルに日付情報がある場合は、

（１）固定的にキーの有効期間を決める。パソコンは日時を管理できるため、キー配信時に日付情報も同時に送り、音声再生装置は日付も記憶しておき、音楽ファイルの再生時にそのファイルの作成された日付と比較して、有効期間を超える場合にはキーの更新を要求する。この方法では必ず一定期日毎にキーの更新要求がなされ、古くなったファイルの再生はしないという正規の使用方法に従っているユーザーに対してもキー更新という煩わしい作業を強いることになり好ましくない。しかし、最も単純で簡単な方法である。

【００６７】（２）再生するファイルの日付によって、有効期日を自動的に延長する。

【００６８】音楽ファイルを再生するときに、ファイルの作成日付を調べ、音声再生装置に記憶してある日付と比較し、新しければ内部に記憶してある日付を最新ファイルの日付に更新する。再生を指定されたファイルの日付と、内部に記憶している日付を比較し、有効期間以上の隔たりがある場合に、キーの更新を要求する。

【００６９】ここでファイルの作成日付の最新値ではなく、いくつかのファイルの作成日付の平均値を取る方法もある。ただし、日付が過去に戻らないような制限を付ける必要もある。

【００７０】ファイルに日付情報がない場合は、

（３）再生回数または総再生時間で管理する。再生回数または再生時間を記憶しておき、逐次更新して、所定の回数または時間になった場合に、キーの更新を要求する。この方法は、(1)と同様に単純ではあるが、定期的にキーの更新要求をするため好ましくない。

【００７１】（４）再生ファイルの識別を行い、再生回数をカウントする。

【００７２】ある特定のデータファイルの再生回数に制限を与えたいのであり、ファイルの識別手段を設けることによって、その目的を達成することができる。

【００７３】例えば、音声再生装置に、再生回数を記憶する配列変数領域を２５６バイト確保し、キー更新時にゼロクリアしておく。ファイルの識別はハッシュ関数（例えばファイルデータの複数の固定アドレスのデータバイトの排他的論理和をとる）で行い、関数値を配列の添え字として、そのカウンタ変数を＋１する。このとき変数値が、最大再生回数の規定値（例えば１００回）を超えた場合に、キーの更新を要求する。

【００７４】ただし、ハッシュ関数では、異なるファイルでも１／２５６の確率で同じ値を返す。多くの曲の再生をしているうちに、識別能力が劣化してくるといえる。このため、定期的に誤識別の回数を補正する必要がある。例えば、非ゼロ値の変数の個数が全体の半数を超えていた（すなわち少なくとも異なる１２８曲の再生を行ったことが明らかである）場合、その非ゼロ値の中で最小の値を、非ゼロのすべての変数から減算するという方法がある。

【００７５】以上の例では、キーの更新要求をするとしたが、単に再生を拒否するだけでもよい。

【００７６】その他、本発明の実施には、以下のような例の適用も可能である。

【００７７】（１）ヘッダ情報の追加

パソコンでは、ファイルの作成日付を簡単に変更できるユーティリティプログラムがありファイルの管理情報の日付は容易に改竄される可能性がある。このため、暗号化されるデータの先頭部にヘッダ情報を付加し、ここに作成日付を入れておくことが有効である。同時に、データの管理責任を明確にするため、ユーザーの個人情報、氏名やログインネームなどもヘッダに容れるようにすることもできる。

【００７８】（２）データの途中からの暗号化

ＣＤリニアＰＣＭデータのまま暗号化すると、殆どすべての音楽データは無音状態で始まっているため、先頭部分のデータはゼロが連続していて、本実施例の暗号化方式では、キー値がそのまま見えてしまうことになる。このような場合は、ファイルの先頭からではなく有効な音声データが確実に存在しているファイルの途中から暗号化を行うことが有効である。

【００７９】（３）再生前のチェック

暗号化されたファイルはキーが不一致の場合は、ノイズ音にしかならない。ユーザーに不快な思いをさせないように、復号が正常になされたことを確認する手段（チェックサムなど）を設け、実際に音楽再生する前にチェックして、ユーザーに通知し音声再生をしないようにもできる。また、データが圧縮されている場合は、圧縮フォ

11

ーマットの正当性を確認することによってチェックを行うこともできる。

【００８０】

【発明の効果】著作物であるＣＤ音楽データの複製、蓄積、転送を、パソコンのデータファイルとして統一的に簡単に扱うことができる。

【００８１】光ディスク装置からアナログ出力の機能を削除することによって、装置の価格を安くできるという副次的な効果もある。

【図面の簡単な説明】

【図１】ＣＤ－ＲＯＭドライブとフラッシュメモリカードとカード型プレーヤで構成されるシステムを示す図。

【図２】ＣＤ－ＲＯＭドライブとハードディスクとサウンドカードで構成されるシステムを示す図。

【図３】暗号・復号化方法を示す図。

12

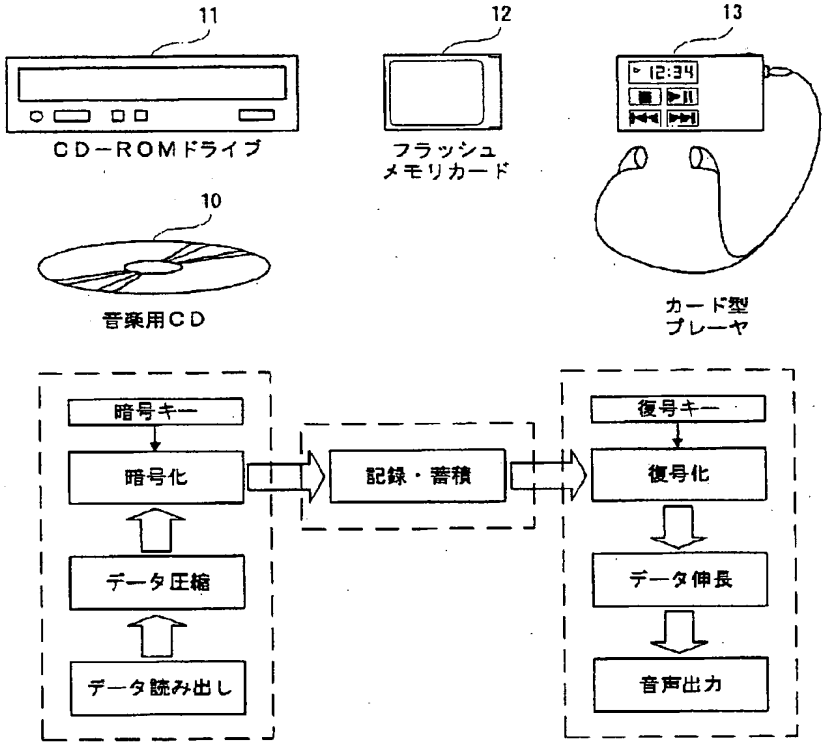
＊【図４】暗号・復号キーの生成と配信方法を説明する図。

【符号の説明】

１０…音楽用ＣＤ、　１１…ＣＤ－ＲＯＭドライブ、１２…フラッシュメモリカード、１３…カード型プレーヤ、２０…音楽用ＣＤ、　２１…ＣＤ－ＲＯＭドライブ、２２…ハードディスクドライブ、　２３…サウンドカード、３１…暗号・復号化用の排他的論理和、３２…３２ビットシフトレジスタ、３３ａ，３３ｂ…フィードバックシフト用の排他的論理和、３４…フィードバックシフトレジスタ法によるＭ系列乱数発生手段、３５…暗号・復号キー、４１…音声再生装置－甲、４２…音声再生装置－乙、４３…光ストレージ装置、４４…キー生成・配信手段（オペレーティングシステム）。

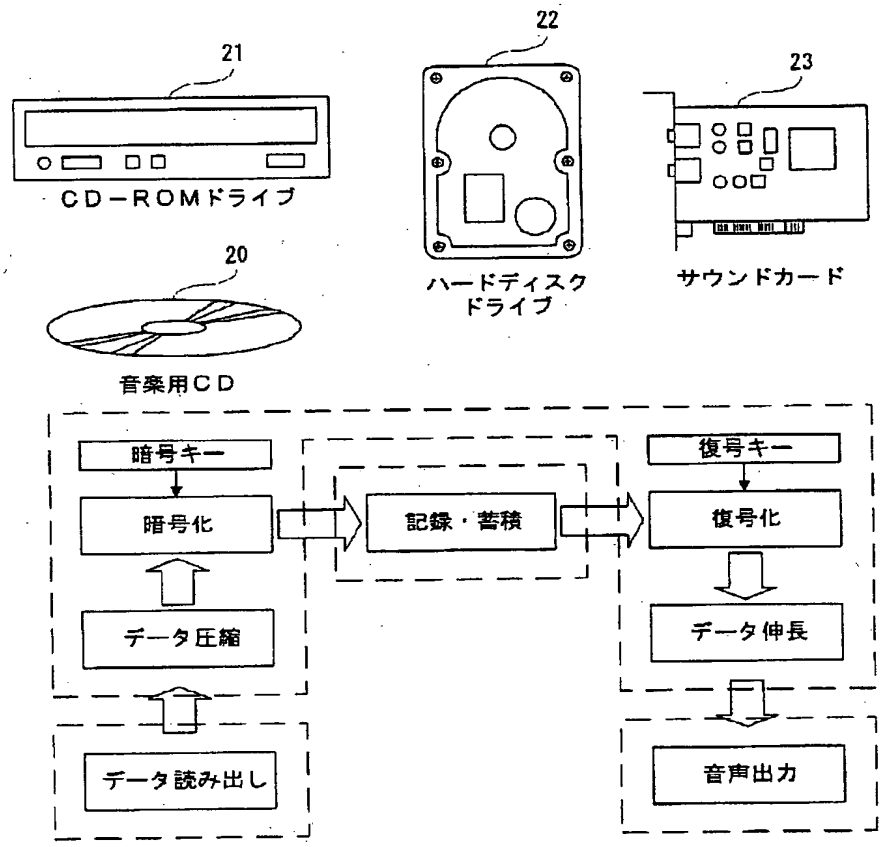
【図１】

図　１



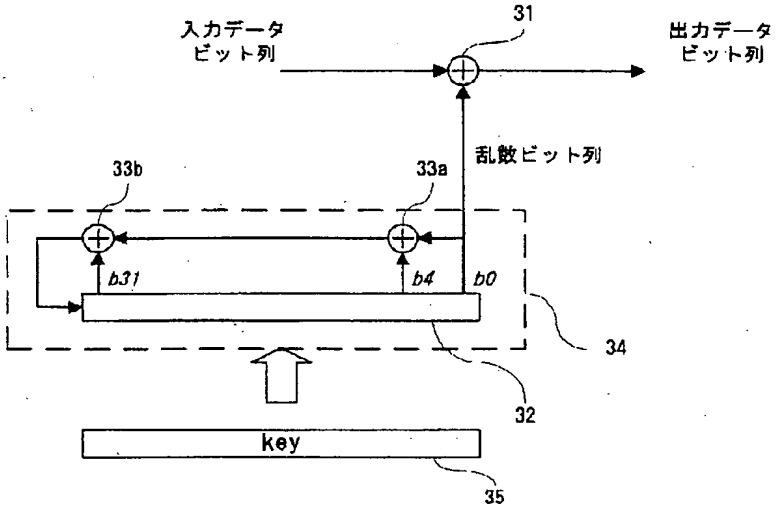
【図２】

図 2


21
CD－ROMドライブ
22
ハードディスク
ドライブ
23
サウンドカード
20
音楽用ＣＤ
暗号キー
暗号化
データ圧縮
データ読み出し
記録・蓄積
復号キー
復号化
データ伸長
音声出力

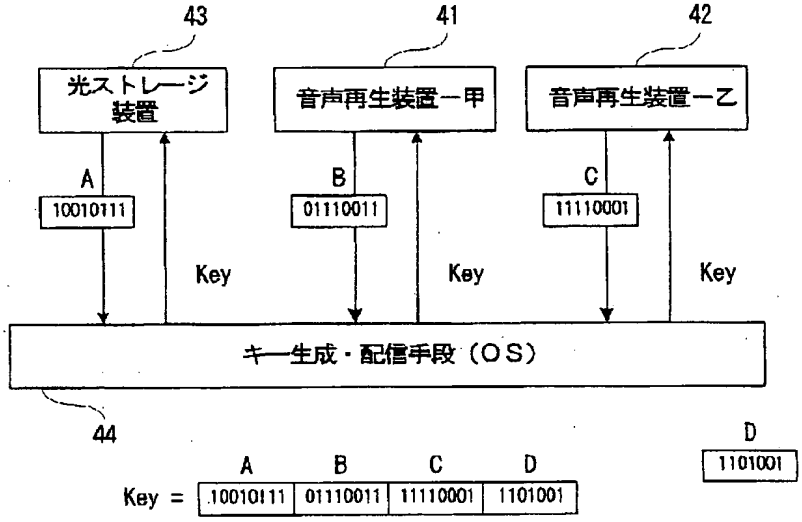
【図３】

図 3


入力データ
ビット列
31
出力データ
ビット列
乱数ビット列
33b
33a
b31
b4
b0
34
32
key
35

【図４】

図 4


43
41
42
光ストレージ
装置
音声再生装置一甲
音声再生装置一乙
A
10010111
B
01110011
C
11110001
Key
Key
Key
キー生成・配信手段（OS）
44
D
1101001
A
B
C
D
Key =
10010111
01110011
11110001
1101001